特　許　協　力　条　約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　ＰＣＴ－１８４５	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０３／０８７９４	国際出願日 （日.月.年）　１０．０７．２００３	優先日 （日.月.年）　０７．１０．２００２
国際特許分類（ＩＰＣ） Ｉｎｔ．Ｃｌ⁷．　Ｇ０９Ｃ１／００，Ｇ０６Ｆ７／５８		
出願人（氏名又は名称） 小林　朗		

１．この報告書は、ＰＣＴ３５条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．この国際予備審査報告は、この表紙を含めて全部で　3　ページからなる。

３．この報告には次の附属物件も添付されている。

a　☒　附属書類は全部で　５２　ページである。

☒　補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第６０７号参照）

☐　第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b　☐　電子媒体は全部で＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、コンピュータ読み取り可能な形式による配列表又は配列表に関連するテーブルを含む。（実施細則第８０２号参照）

４．この国際予備審査報告は、次の内容を含む。

☒　第Ｉ欄　国際予備審査報告の基礎
☐　第Ⅱ欄　優先権
☐　第Ⅲ欄　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☐　第Ⅳ欄　発明の単一性の欠如
☒　第Ⅴ欄　ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐　第Ⅵ欄　ある種の引用文献
☐　第Ⅶ欄　国際出願の不備
☐　第Ⅷ欄　国際出願に対する意見

国際予備審査の請求書を受理した日 ２８．０４．２００４	国際予備審査報告を作成した日 ２４．１１．２００４	
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 石田　悟行	5M　9469
	電話番号　０３－３５８１－１１０１　内線　３５９８	

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００４年1月）

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／０８７９４

第Ⅰ欄　報告の基礎

１．この国際予備審査報告は、下記に示す場合を除くほか、国際出願の言語を基礎とした。

☐ この報告は、＿＿＿＿＿＿ 語による翻訳文を基礎とした。
それは、次の目的で提出された翻訳文の言語である。
☐ ＰＣＴ規則12.3及び23.1(b)にいう国際調査
☐ ＰＣＴ規則12.4にいう国際公開
☐ ＰＣＴ規則55.2又は55.3にいう国際予備審査

２．この報告は下記の出願書類を基礎とした。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☒ 明細書
第 1-3, 14-17, 28 ページ、 出願時に提出されたもの
第 4-13, 18-27/1, 29-36 ページ*、２７．０９．２００４ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿＿＿ ページ*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 請求の範囲
第 2-4, 6, 13, 20 項、 出願時に提出されたもの
第 ＿＿＿＿＿＿ 項*、ＰＣＴ１９条の規定に基づき補正されたもの
第 1, 5, 7, 8-12, 14-19 項*、２７．０９．２００４ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿＿＿ 項*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☒ 図面
第 3, 5-7, 9-11, 13-18 ~~ページ~~／図、 出願時に提出されたもの
第 1, 2, 4, 8, 12 ~~ページ~~／図*、２７．０９．２００４ 付けで国際予備審査機関が受理したもの
第 ＿＿＿＿＿＿ ページ／図*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

３．☐ 補正により、下記の書類が削除された。

☐ 明細書　第＿＿＿＿＿＿ ページ
☐ 請求の範囲　第＿＿＿＿＿＿ 項
☐ 図面　第＿＿＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）＿＿＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿

４．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

☐ 明細書　第＿＿＿＿＿＿ ページ
☐ 請求の範囲　第＿＿＿＿＿＿ 項
☐ 図面　第＿＿＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）＿＿＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿

＊ ４．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ０３／０８７９４

第Ⅴ欄　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（N）	請求の範囲	１－２０	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲	１－２０	有
	請求の範囲		無
産業上の利用可能性（ＩＡ）	請求の範囲	１－２０	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

請求の範囲１乃至２０に係る発明は、国際調査報告で引用したいずれの文献にも記載されておらず、当業者にとって自明なものでもない。

体のスループットが低下するという問題があり、ソフトウエアでは使用することが困難であった。

また、疑似乱数の暗号強度を十分に確保するためには、線形フィードバックシフトレジスタ１０３のシフトレジスタ１０５の数や、線形フィードバックシフトレジスタ１０３の個数をある程度の数以上必要とする。しかし、スループットは、線形フィードバックシフトレジスタ１０３のシフトレジスタ１０５の数が増加するほど、或いは線形フィードバックシフトレジスタ１０３の個数が増加するほど低くなるという、相反する関係にある。したがって、高い暗号強度を確保しつつ、高いスループットを実現することは困難であった。

本発明は、上述の第１及び第２の解決課題の少なくとも一方を解決すべくなされたものであり、その目的は、強い暗号強度を維持しつつ線形フィードバックシフトレジスタの構成を容易かつ動的に変更することができ、また、十分に高い暗号強度を確保しつつ、より高いスループットを実現できる疑似乱数発生方法等を提供することにある。

［課題を解決するための手段］

上記課題を解決する請求項１に記載の発明による疑似乱数発生方法は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタの初期値を設定する第１ステップと、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める第２ステップと、導出値と線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値とを乗算して、線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出する第３ステップと、その算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させる第４ステップと、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する第５ステップと、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成する第６ステップと、再構成した後の線形フィードバックシフトレジスタから初期値をもとに疑似乱数を発生させる第７ステップと、を有することを特徴とする。

この発明は、出力系列がM系列のビット列をｓ個ごとにサンプルしたビット列は、そのM系列の１周期分のビット数（＝（２＾ｎ）－１）と導出値が互いに素であるときには、他の構成を有する線形フィードバックシフトレジスタのM系列を構成し、また、少なくとも２周期分以上のビット数を有するビット列から線形フィードバックシフトレジスタを求めることができることを利用するものである。

この発明によると、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタの初期値を設定し、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める。

そして、導出値と線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値とを乗算して、線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出し、その算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させ、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する。

そして、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成し、再構成した後の線形フィードバックシフトレジスタから初期値をもとに疑似乱数を発生させる。

これによれば、線形フィードバックシフトレジスタの構成を初期値に基づいて動的に変更することができ、変更後の線形フィードバックシフトレジスタからM系列のビット列を出力させることができる。したがって、解読者は、疑似乱数発生器から出力される疑似乱数に基づいて再構成前の線形フィードバックシフトレジスタの構成を得ることができず、初期値や秘密鍵も解読することができない。この結果、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

請求項２の発明は、請求項１に記載の疑似乱数発生方法において、初期値に対してハッシュ関数を施してハッシュ値を求め、そのハッシュ値に最も近似した素数を導出値として採用することを特徴とする。

この発明によると、初期値に対してハッシュ関数を施してハッシュ値を求め、そのハッシュ値に最も近似した素数を導出値として採用するので、導出値の推定困難度を高めることができ、より高度な秘匿性を得ることができる。

請求項３の発明は、請求項１または２に記載の疑似乱数発生方法において、線形フィードバックシフトレジスタの再構成は、バーレイキャンプマッセイアルゴリズムを用いて行われることを特徴とする。

この発明は、少なくとも２周期分以上のビット数を有するビット列から線形フィードバックシフトレジスタを求めることができるという、バーレイキャンプマッセイアルゴリズムを利用するものである。

請求項４の発明は、請求項１～３のいずれかに記載の疑似乱数発生方法において、第６ステップの発明は、発生させた疑似乱数を非線形変換する第７ステップを有することを特徴とする。この発明によると、発生させた疑似乱数を非線形変換するので、疑似乱数に非線形性を与えることができ、暗号強度を更に向上させることができる。

請求項５に記載の発明による疑似乱数発生器は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタと、秘密鍵に基づき線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める導出値算出手段と、線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値と導出値とを乗算して、線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、その算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させるビット列出力手段と、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、再構成後の線形フィードバックシフトレジスタから初期値をもとに疑似乱数を発生させる疑似乱数発生手段と、を有することを特徴とする。

この発明は、出力系列がM系列のビット列をｓ個ごとにサンプルしたビット列は、そのM系列の１周期分のビット数（＝（２＾ｎ）－１）と導出値ｓが互いに素であるときには、他の構成を有する線形フィードバックシフトレジスタのM系

列を構成し、また、少なくとも２周期分以上のビット数を有するビット列から線形フィードバックシフトレジスタを求めることができることを利用するものである。

この発明によると、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタの初期値を設定し、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める。

そして、導出値と線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値とを乗算して、線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出し、その算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させ、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する。

そして、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成し、再構成した後の線形フィードバックシフトレジスタから初期値をもとに疑似乱数を発生させる。

これによれば、線形フィードバックシフトレジスタの構成を初期値に基づいて動的に変更することができ、変更後の線形フィードバックシフトレジスタからＭ系列のビット列を出力させることができる。したがって、解読者は、疑似乱数発生器から出力される疑似乱数に基づいて再構成前の線形フィードバックシフトレジスタの構成を得ることができず、初期値や秘密鍵も解読することができない。この結果、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

請求項６に記載の発明は、請求項５に記載の疑似乱数発生器において、線形フィードバックシフトレジスタ再構成手段の代わりに、新ビット列を出力可能な構成を有する第２の線形フィードバックシフトレジスタを生成する線形フィードバックシフトレジスタ生成手段を設け、疑似乱数発生手段は、第２の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させることを特徴とする。この発明によると、線形フィードバックシフトレジスタを再構成前の線形フィードバックシフトレジスタと第２の線形フィードバックシフトレジスタの２つに分けることができ、より秘匿性の向上を図ることができる。

請求項７に記載の発明による疑似乱数発生器は、秘密鍵に基づいて所定のビット数を有する選択用乱数ビット列を出力する乱数ビット列出力部と、乱数ビット列出力部から出力された選択用乱数ビット列に基づいて選択用乱数ビット列のビット数よりも大きなビット数を有する増幅乱数ビット列を出力する乱数ビット列増幅部と、乱数ビット列増幅部から出力された増幅乱数ビット列を非線形変換して疑似乱数を出力する非線形変換部とを有し、乱数ビット列出力部は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタと、秘密鍵に基づき線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める導出値算出手段と、線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値と導出値とを乗算して、線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させるビット列出力手段と、ビット列出力手段から出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、線形フィードバックシフトレジスタ再構成手段によって再構成された再構成後の線形フィードバックシフトレジスタを用いて初期値をもとに選択用乱数ビット列を出力する選択用乱数ビット列出力手段とを有し、乱数ビット列増幅部は、選択用乱数ビット列よりも大きなビット数を有する増幅乱数ビット列を予め複数格納した乱数テーブルと、選択用乱数ビット列出力手段から出力された選択用乱数ビット列を用いて乱数テーブルを参照することにより、乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択可能な増幅乱数ビット列選択手段とを有し、非線形変換部は、増幅乱数ビット列選択手段により選択された増幅乱数ビット列を非線形関数によって非線形変換し疑似乱数として出力する非線形変換手段とを有することを特徴とする。

この発明は、出力系列がM系列のビット列をｓ個ごとにサンプルしたビット列

は、そのM系列の１周期分のビット数（＝（２＾ｎ）－１）と導出値ｓが互いに素であるときには、他の構成を有する線形フィードバックシフトレジスタのM系列を構成し、また、少なくとも２周期分以上のビット数を有するビット列から線形フィードバックシフトレジスタを求めることができることを利用するものである。

この発明によると、疑似乱数発生器は、秘密鍵に基づいて所定のビット数を有する選択用乱数ビット列を出力する乱数ビット列出力部と、その選択用乱数ビット列に基づいて選択用乱数ビット列のビット数よりも大きなビット数を有する増幅乱数ビット列を出力する乱数ビット列増幅部と、その増幅乱数ビット列を非線形変換して疑似乱数を出力する非線形変換部を有している。

乱数ビット列出力部は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタを有しており、その線形フィードバックシフトレジスタの初期値を秘密鍵に基づいて設定し、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める。

そして、導出値と線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値とを乗算して、線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出し、その算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させ、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する。

それから、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成し、再構成した後の線形フィードバックシフトレジスタから初期値をもとに選択用乱数ビット列を出力させる。

乱数ビット列増幅部は、選択用乱数ビット列よりも大きなビット数を有する増幅乱数ビット列を予め複数格納した乱数テーブルを有しており、乱数ビット列出力部から出力された選択用乱数ビット列を用いて乱数テーブルを参照することにより、乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択する。

非線形変換部は、乱数ビット列増幅部の増幅乱数ビット列選択手段により選択

された増幅乱数ビット列を非線形変換して疑似乱数として出力する。

これによれば、M系列の選択用乱数ビット列を出力する線形フィードバックシフトレジスタの構成を初期値に基づいて動的に変更することができ、変更後の線形フィードバックシフトレジスタから新たなM系列の選択用乱数ビット列を出力させることができる。したがって、解読者は、疑似乱数発生器から出力される疑似乱数に基づいて再構成前の線形フィードバックシフトレジスタの構成を得ることができず、初期値や秘密鍵も解読することができない。この結果、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

また、乱数ビット列出力部から出力された選択用乱数ビット列を用いて乱数テーブルを参照し、乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択することによって、小さなビット列を有する選択用乱数ビット列に基づいて、より大きなビット数を有する増幅乱数ビット列を得ることができる。

したがって、非線形変換手段に入力される乱数ビット列をより大きなビット数を有するものにすることができる。これにより、従来、ボトルネックとなっていた非線形変換手段よりも上流側の乱数ビット列を出力する部分のスループットを向上させ、非線形変換手段のスループットに近づけることができ、疑似乱数発生器全体のスループットを高速化することができる。

請求項8に記載の発明は、請求項7に記載の疑似乱数発生器において、乱数ビット列増幅部は、秘密鍵が与えられることにより秘密鍵に基づいて前記増幅乱数ビット列を発生させる増幅乱数ビット列発生手段と、増幅乱数ビット列発生手段により発生させた増幅乱数ビット列を乱数テーブルに格納して、乱数テーブルの初期設定を行う乱数テーブル初期設定手段を有することを特徴とする。

この発明によると、秘密鍵が与えられることにより秘密鍵に基づいて増幅乱数ビット列を発生させ、乱数テーブルに格納して、乱数テーブルの初期設定を行うので、秘密鍵を変更するごとに乱数テーブル内の初期値を変更することができる。したがって、暗号強度を増大させることができる。

請求項9に記載の発明は、請求項7または8に記載の疑似乱数発生器において、

乱数ビット列出力部は、選択用乱数ビット列出力手段が複数設けられ、乱数ビット列増幅部は、乱数テーブルが各選択用乱数ビット列出力手段にそれぞれ対応するように設けられ、増幅乱数ビット列選択手段が各選択用乱数ビット列出力手段から各々出力された各選択用乱数ビット列を用いて各選択用乱数ビット列出力手段ごとに対応する乱数テーブルをそれぞれ参照し、各乱数テーブル内からそれぞれ該当する増幅乱数ビット列を選択し、非線形変換部は、非線形変換手段が各増幅乱数ビット列選択手段によって各乱数テーブルから選択された各増幅乱数ビット列を用いて非線形関数により非線形変換し疑似乱数として出力することを特徴とする。

この発明によると、乱数ビット列出力部の各選択用乱数ビット列出力手段からそれぞれ選択用乱数ビット列が出力され、これらの各選択用乱数ビット列を用いて各乱数テーブルがそれぞれ参照される。そして、その参照により各乱数テーブルから選択された各増幅乱数ビット列を用いて非線形変換部の非線形変換手段が非線形関数により非線形変換することによって疑似乱数を発生させる。

したがって、従来はボトルネックとなっていた非線形変換手段よりも上流側の乱数ビット列を出力する部分のスループットを向上させることができ、疑似乱数発生器全体のスループットを高速化することができる。

請求項１０に記載の発明は、請求項９に記載の疑似乱数発生器において、乱数ビット列増幅部は、各選択用乱数ビット列出力手段ごとにそれぞれ複数の乱数テーブルを設け、増幅乱数ビット列選択手段により各乱数テーブル内から選択された各増幅乱数ビット列を乱数ビット列出力部の選択用乱数ビット列出力手段ごとに排他的論理和演算して非線形変換部の非線形変換手段に出力する排他的論理和演算処理手段を有することを特徴とする。

この発明によると、各乱数テーブルから選択された各増幅乱数ビット列が選択用乱数ビット列出力手段ごとに排他的論理和演算してから非線形変換手段に出力されるので、増幅乱数ビット列発生手段によって発生させた乱数ビット列をそのまま用いたものよりも、暗号強度を増大させることができる。

請求項１１に記載の発明は、請求項９または１０に記載の疑似乱数発生器において、乱数ビット列増幅部は、所定のタイミングで各乱数テーブル同士の入れ替

えを行う乱数テーブル入れ替え手段を有することを特徴とする。

この発明によると、乱数ビット列増幅部は、所定のタイミングで各乱数テーブル同士の入れ替えを行うので、参照元となる乱数テーブルを変更することができる。したがって、固定さ

れたものよりも暗号強度を増大させることができる。

請求項１２に記載の発明は、請求項１１に記載の疑似乱数発生器において、乱数テーブル入れ替え手段が、各乱数テーブルを参照するために必要な選択用乱数ビット列を選択用乱数ビット列出力手段が出力するごとに、各乱数テーブル同士の入れ替えを行うことを特徴とする。

この発明は、上述の請求項に記載した所定のタイミングの一具体例を示したものである。これによると、各乱数テーブルを参照するために必要な選択用乱数ビット列を選択用乱数ビット列出力手段が出力するごとに各乱数テーブル同士の入れ替えを行う。したがって、短いサイクルで参照元となる乱数テーブルを変更することができ、暗号強度を更に増大させることができる。

請求項１３に記載の発明は、請求項１１または１２に記載の疑似乱数発生器において、乱数テーブル入れ替え手段は、各乱数テーブルの個数と等しい個数の乱数テーブル入れ替え用乱数を発生させ、乱数テーブル入れ替え用乱数を乱数テーブルのテーブル番号として各乱数テーブルに付与し、テーブル番号をもとに予め設定された規則に従って乱数テーブルの順番を入れ替えることを特徴とする。

この発明は、上述の乱数テーブル入れ替え手段についての具体的な一例を示したものである。これによると、乱数テーブル入れ替え用乱数を発生させ、乱数テーブルのテーブル番号として各乱数テーブルに付与し、その付与したテーブル番号をもとに乱数テーブルの順番を入れ替える。したがって、乱数テーブルの順番を簡単かつ迅速に入れ替えることができ、非線形変換手段よりも上流側のスループットを向上させ、非線形変換手段のスループットに近づけることができ、疑似乱数発生器全体のスループットを高速化することができる。

請求項１４に記載の発明は、秘密鍵に基づいて所定のビット数を有する選択用乱数ビット列を出力する乱数ビット列出力部と、乱数ビット列出力部から出力された選択用乱数ビット列に基づいて選択用乱数ビット列のビット数よりも大きなビット数を有する増幅乱数ビット列を出力する乱数ビット列増幅部と、乱数ビット列増幅部から出力された増幅乱数ビット列を非線形変換して疑似乱数を出力する非線形変換部として機能させるための疑似乱数発生プログラムであって、乱数ビット列出力部は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾

n）－１個となるビット列を出力可能な線形フィードバックシフトレジスタと、秘密鍵に基づき線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める導出値算出手段と、線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値と導出値とを乗算して、線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、ビット数算出手段により算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させるビット列出力手段と、ビット列出力手段から出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、線形フィードバックシフトレジスタ再構成手段によって再構成された再構成後の線形フィードバックシフトレジスタを用いて選択用乱数ビット列を出力する選択用乱数ビット列出力手段とを有し、乱数ビット列増幅部は、選択用乱数ビット列よりも大きなビット数を有する増幅乱数ビット列を予め複数格納した乱数テーブルと、選択用乱数ビット列出力手段から出力された選択用乱数ビット列を用いて乱数テーブルを参照することにより、乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択可能な増幅乱数ビット列選択手段とを有し、非線形変換部は、増幅乱数ビット列選択手段により選択された増幅乱数ビット列を非線形関数によって非線形変換し疑似乱数として出力する非線形変換手段を有することを特徴とする。

この発明は、出力系列がM系列のビット列をｓ個ごとにサンプルしたビット列は、そのM系列の１周期分のビット数（＝（２＾ｎ）－１）と導出値ｓが互いに素であるときには、他の構成を有する線形フィードバックシフトレジスタのM系列を構成し、また、少なくとも２周期分以上のビット数を有するビット列から線形フィードバックシフトレジスタを求めることができることを利用するものである。

この発明によると、疑似乱数発生器は、秘密鍵に基づいて所定のビット数を有

する選択用乱数ビット列を出力する乱数ビット列出力部と、その選択用乱数ビット列に基づいて選択用乱数ビット列のビット数よりも大きなビット数を有する増幅乱数ビット列を出力する乱数ビット列増幅部と、その増幅乱数ビット列を非線形変換して疑似乱数を出力する非線形変換部を有している。

乱数ビット列出力部は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタを有しており、その線形フィードバックシフトレジスタの初期値を秘密鍵に基づいて設定し、所定の演算処理により初期値から線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める。

そして、導出値と線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値とを乗算して、線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出し、その算出したビット数分のビット列を線形フィードバックシフトレジスタから初期値をもとに出力させ、その出力したビット列から導出値の間隔ごとにビット列を取り出して新ビット列を生成する。

それから、その新ビット列を出力可能な構成に線形フィードバックシフトレジスタの構成を再構成し、再構成した後の線形フィードバックシフトレジスタから初期値をもとに選択用乱数ビット列を出力させる。

乱数ビット列増幅部は、選択用乱数ビット列よりも大きなビット数を有する増幅乱数ビット列を予め複数格納した乱数テーブルを有しており、乱数ビット列出力部から出力された選択用乱数ビット列を用いて乱数テーブルを参照することにより、乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択する。

非線形変換部は、乱数ビット列増幅部の増幅乱数ビット列選択手段により選択された増幅乱数ビット列を非線形変換して疑似乱数として出力する。

これによれば、Ｍ系列の選択用乱数ビット列を出力する線形フィードバックシフトレジスタの構成を初期値に基づいて動的に変更することができ、変更後の線形フィードバックシフトレジスタから新たなM系列の選択用乱数ビット列を出力させることができる。したがって、解読者は、疑似乱数発生器から出力される疑似乱数に基づいて再構成前の線形フィードバックシフトレジスタの構成を得るこ

とができず、初期値や秘密鍵も解読することができない。この結果、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

また、乱数ビット列出力部から出力された選択用乱数ビット列を用いて乱数テーブルを参照し、乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択することによって、小さなビット列を有する選択用乱数ビット列に基づいて、より大きなビット数を有する増幅乱数ビット列を得ることができる。

したがって、非線形変換手段に入力される乱数ビット列をより大きなビット数を有するものにすることができる。これにより、従来、ボトルネックとなっていた非線形変換手段よりも上流側の乱数ビット列を出力する部分のスループットを向上させ、非線形変換手段のスループットに近づけることができ、疑似乱数発生器全体のスループットを高速化することができる。

請求項１５に記載の発明は、請求項１４に記載の疑似乱数発生プログラムにおいて、乱数ビット列増幅部は、秘密鍵が与えられることにより秘密鍵に基づいて増幅乱数ビット列を発生させ、乱数テーブルに格納して、乱数テーブルの初期設定を行う乱数テーブル初期設定手段としてコンピュータを機能させることを特徴とする。

この発明によると、秘密鍵が与えられることにより秘密鍵に基づいて増幅乱数ビット列を発生させ、乱数テーブルに格納して、乱数テーブルの初期設定を行うので、秘密鍵を変更するごとに乱数テーブル内の初期値を変更することができる。したがって、暗号強度を増大させることができる。

請求項１６に記載の発明は、請求項１４または１５に記載の疑似乱数発生プログラムにおいて、乱数ビット列出力部は、選択用乱数ビット列出力手段が複数設けられ、乱数ビット列増幅部は、乱数テーブルが各選択用乱数ビット列出力手段にそれぞれ対応するように設けられ、増幅乱数ビット列選択手段が各選択用乱数ビット列出力手段から各々出力された各選択用乱数ビット列を用いて各選択用乱数ビット列出力手段ごとに対応する乱数テーブルをそれぞれ参照し、各乱数テーブル内からそれぞれ該当する増幅乱数ビット列を選択し、非線形変換部は、非線形変換手段が各増幅乱数ビット列選択手段によって各乱数

テーブルから選択された各増幅乱数ビット列を用いて非線形関数により非線形変換し疑似乱数として出力することを特徴とする。

この発明によると、乱数ビット列出力部の各選択用乱数ビット列出力手段からそれぞれ選択用乱数ビット列が出力され、乱数ビット列増幅部では、各選択用乱数ビット列を用いて各乱数テーブルがそれぞれ参照され、その参照により各乱数テーブルから選択された各増幅乱数ビット列を用いて非線形変換部の非線形変換手段が非線形関数により非線形変換することによって疑似乱数を発生させる。

したがって、従来はボトルネックとなっていた非線形変換手段よりも上流側の乱数ビット列を出力する部分のスループットを向上させ、非線形変換手段のスループットに近づけることができ、疑似乱数発生器全体のスループットを高速化することができる。

請求項１７に記載の発明は、請求項１６に記載の疑似乱数発生プログラムにおいて、乱数ビット列増幅部は、各選択用乱数ビット列出力手段ごとにそれぞれ複数の乱数テーブルを設け、増幅乱数ビット列選択手段により各乱数テーブル内から選択された各増幅乱数ビット列を乱数ビット列出力部の選択用乱数ビット列出力手段ごとに排他的論理和演算して非線形変換部の非線形変換手段に出力する排他的論理和演算処理手段としてコンピュータを機能させることを特徴とする。

この発明によると、各乱数テーブルから選択された各増幅乱数ビット列が選択用乱数ビット列出力手段ごとに排他的論理和演算してから非線形変換手段に出力されるので、増幅乱数ビット列発生手段によって発生させた乱数ビット列をそのまま用いたものよりも、暗号強度を増大させることができる。

請求項１８に記載の発明は、請求項１６または１７に記載の疑似乱数発生プログラムにおいて、乱数ビット列増幅部は、所定のタイミングで前記各乱数テーブル同士の入れ替えを行う乱数テーブル入れ替え手段としてコンピュータを機能させることを特徴とする。

この発明によると、乱数ビット列増幅部は、所定のタイミングで各乱数テーブル同士の入れ替えを行うので、参照元となる乱数テーブルを変更することができる。したがって、乱数テーブルが固定されているものよりも暗号強度を増大させることができる。

請求項１９に記載の発明は、請求項１８に記載の疑似乱数発生プログラムにおいて、乱数テーブル入れ替え手段は、各乱数テーブルを参照するために必要な選択用乱数ビット列を乱数ビット列出力部の選択用乱数ビット列出力手段が出力するごとに、各乱数テーブル同士の入れ替えを行うことを特徴とする。

この発明は、上述の請求項に記載した所定のタイミングの一具体例を示したものである。これによると、乱数ビット列出力部は、各乱数テーブルを参照するために必要な選択用乱数ビット列を選択用乱数ビット列出力手段が出力するごとに各乱数テーブル同士の入れ替えを行う。したがって、短いサイクルで参照元となる乱数テーブルを変更することができ、暗号強度を更に増大させることができる。

請求項２０に記載の発明は、請求項１８または１９に記載の疑似乱数発生プログラムにおいて、乱数テーブル入れ替え手段は、各乱数テーブルの個数と等しい個数の乱数テーブル入れ替え用乱数を発生させ、乱数テーブル入れ替え用乱数を乱数テーブルのテーブル番号として各乱数テーブルに付与し、テーブル番号をもとに予め設定された規則に従って乱数テーブルの順番を入れ替えることを特徴とする。

この発明は、上述の乱数テーブル入れ替え手段についての具体的な一例を示したものである。これによると、乱数テーブル入れ替え用乱数を発生させ、乱数テーブルのテーブル番号として各乱数テーブルに付与し、その付与したテーブル番号をもとに乱数テーブルの順番を入れ替える。したがって、乱数テーブルの順番を簡単かつ迅速に入れ替えることができ、非線形変換手段よりも上流側のスループットを向上させ、非線形変換手段のスループットに近づけることができ、疑似乱数発生器全体のスループットを高速化することができる。

[発明の実施の形態]

（第１の実施の形態）

次に、本発明の第１の実施の形態について図に基づいて説明する。

第１図は、本実施の形態における疑似乱数発生器１を説明する図である。本実施の形態では、非線形コンバイナ型の疑似乱数発生器１を例に説明する。

疑似乱数発生器１は、利用者から与えられる秘密鍵に基づいて初期値を設定する初期値設定部（図示せず）と、初期値設定部から受け取った初期値をもとに疑似乱数を生成する複数の疑似乱数生成部１０と、これら複数の疑似乱数生成部１０の出力側に各々接続され、各疑似乱数生成部１０から出力される疑似乱数を非線形変換する非線形変換部２０を有している。

初期値設定部は、利用者から与えられる秘密鍵をビット列に変換し、疑似乱数

換される（ステップＳ８）。これにより、疑似乱数に非線形性を与えることができ、暗号強度を更に向上させることができる。

上記構成を有する疑似乱数発生器１によれば、線形フィードバックシフトレジスタ１１の構成を初期値に基づいて容易かつ動的に変更することができ、変更後もM系列を出力させることができる。したがって、解読者は、再構成前の線形フィードバックシフトレジスタの構成を取得することができない。これにより、従来、線形フィードバックシフトレジスタの構成が既知であることを前提に成り立っていた既存の暗号解読法は、成立しなくなる。したがって、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

尚、上述の実施の形態では、非線形コンバイナ型の疑似乱数発生器１を例に説明したが、非線形コンバイナ型に限定されるものではなく、線形フィードバックシフトレジスタを用いる疑似乱数発生器であればよく、例えばブロック型暗号方式に用いられる疑似乱数発生器に用いてもよい。

また、上記のステップＳ６で、新ビット列に基づいて線形フィードバックシフトレジスタ１１の構成を再構成する代わりに、新ビット列を出力可能な構成を有する第２の線形フィードバックシフトレジスタを生成し、ステップＳ７で、その第２の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させてもよい。これによれば、線形フィードバックシフトレジスタを２つに分けることができ、より秘匿性の向上を図ることができる。また、第１の実施の形態における疑似乱数発生器１は、ソフトウエアやハードウエアのいずれによって構成してもよい。

（第２の実施の形態）

次に、本発明の第２の実施の形態について図に基づいて説明する。

第４図は、第２の実施の形態における疑似乱数発生器２の原理を示す説明図である。本実施の形態における疑似乱数発生器２は、疑似乱数発生プログラムをコンピュータハードウエア上で実行することによって実現される非線形コンバイナ型の疑似乱数発生器２である。尚、本実施の形態では、暗号化装置（従来技術を参照）に組み込まれた場合のものを例に説明し、復号化装置のものについては同様であるのでその詳細な説明を省略する。

疑似乱数発生器２は、第４図に示すように、乱数ビット列出力部５０と、乱数ビット列増幅部６０と、非線形変換部７０を有している。乱数ビット列出力部５０は、α個の選択用乱数ビット列出力手段５１を備えている。選択用乱数ビット列出力手段５１_{1}～５１_{α}は、利用者から与えられるＬｋビットの秘密鍵ＫをもとにＮｉビットを有する選択用乱数ビット列を連続して出力するものであり、例えば線形フィードバックシフトレジスタによって構成される。

乱数ビット列増幅部６０は、Ｎｉビットの選択用乱数ビット列を与えることによりＮｉビットよりも大きなビット数であるＮｏビットの増幅乱数ビット列を出力するように構成されており、乱数テーブル部６１と排他的論理和演算処理手段６３を備えている。

乱数テーブル部６１は、（２＾Ｎｉ）個の乱数ビット列を格納したα×β（以下、単に「αβ」と記す）個の乱数テーブル６２によって構成されている。そして、第４図に示すように、各選択用乱数ビット列出力手段５１ごとにβ（複数）個の乱数テーブル６２が対応するように設けられている。第５図は、一の乱数テーブルの構成を説明する概略図である。各乱数テーブル６２は、第５図に示すように、（２＾Ｎｉ）個でかつ０～（２＾Ｎｉ）－１のインデックス番号が付与されたインデックス部Ｒｉと、各インデックス番号に一対一で対応して設けられ上述の増幅乱数ビット列を格納可能なビット列格納部Ｒｏを有している。

そして、乱数ビット列出力部５０の選択用乱数ビット列出力手段５１から出力された選択用乱数ビット列を引数として、該当するインデックス部Ｒｉのインデックス番号を選択し、そのインデックス番号に対応する乱数ビット列格納部ＲｏからＮｏビットの増幅乱数ビット列を選択できるように構成されている。

排他的論理和演算処理手段６３は、乱数テーブル６２_{1}～$６２_{\alpha\beta}$の参照によって抽出されたαβ個の増幅乱数ビット列を各選択用乱数ビット列出力手段５１ごとに排他的論理和演算処理し、α個の増幅乱数ビット列とし、非線形変換部７０に出力するように構成されている。これにより、乱数テーブル６２_{1}～$６２_{\alpha\beta}$から読み出した増幅乱数ビット列をそのまま非線形変換部７０に出力するのではなく、暗号強度が増幅乱数ビット列そのものに依存することを防止し、暗号強度を更に向上させている。

第６図は、乱数ビット列増幅部６０内に構成される各構成要素を説明する原理図である。上述の乱数ビット列増幅部６０は、第６図に示すように、その内部機構として増幅乱数ビット列選択手段６４を備えている。増幅乱数ビット列選択手段６４は、各選択用乱数ビット列出力手段５１$_1$～５１$_\alpha$から出力された選択用乱数ビット列を引数として各乱数テーブル６２$_1$～６２$_{\alpha\beta}$をそれぞれ参照し、引数と等しい値を有するインデックス番号に対応するビット列格納部Ｒｏから増幅乱数ビット列をそれぞれ選択するように構成されている。

また、乱数ビット列増幅部６０は、乱数テーブル部６１の初期設定を行う乱数テーブル初期設定手段６５と、その乱数テーブル初期設定手段６５により乱数テーブル部６１内に設定される増幅乱数ビット列を発生させる増幅乱数ビット列発生手段６６を備えている。

乱数テーブル初期設定手段６５は、増幅乱数ビット列発生手段６６によって発生させた乱数ビット列をＮｏビットごとに分割して各乱数テーブル６２$_1$～６２$_{\alpha\beta}$の全ての乱数ビット列格納部Ｒｏに格納する処理を行うものであり、本実施の形態では、第１番目の選択用乱数ビット列出力手段５１$_1$に対応する乱数テーブル６２$_1$から第α番目の選択用乱数ビット列出力手段５１$_\alpha$に対応する乱数テーブル６２$_{\alpha\beta}$まで順番に格納するように構成されている。

増幅乱数ビット列発生手段６６は、秘密鍵Ｋをもとに乱数ビット列を出力するものであり、本実施の形態では、ＲＣ４　Ｓｙｐｐｅｔｒｉｃ　Ｓｔｒｅａｐ　Ｃｉｐｈｅｒ（ＲＳＡ　Ｄａｔａ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃ．製）を用いている。しかし、通常の線形フィードバックシフトレジスタなどの疑似乱数ビット列を高速に出力できるもの（主としてストリーム型暗号）であれば他のものであってもよい。

また、第６図に示すように、乱数ビット列増幅部６０は、所定のタイミングで乱数テーブル６２$_1$～６２$_{\alpha\beta}$の順番を入れ替える処理を行う乱数テーブル順番入れ替え手段６７と、その乱数テーブル順番入れ替え手段６７が乱数テーブルの順番入れ替え処理を行うために使用する順番入れ替え用乱数を発生させる入れ替え用乱数発生手段６８を備えている。

乱数テーブル順番入れ替え手段６７は、入れ替え用乱数発生手段６８により発

生さ

せた入れ替え用乱数を、乱数テーブルのテーブル番号として、その発生させた順番で各乱数テーブル62_1～$62_{\alpha\beta}$に順次付与し、その付与した乱数をもとに乱数テーブルの順番を入れ替える処理を行い、乱数テーブル部６１内の増幅乱数ビット列の順番をテーブル単位で変更する。

入れ替え用乱数発生手段６８は、任意の秘密鍵Ｋ０をもとに乱数テーブル入れ替え用乱数を発生させる処理を行うものであり、乱数ビット列出力部５０からＮｉビットを有するα個の選択用乱数ビット列を入力するごとに、αβ個の入れ替え用乱数を発生するように構成されている。任意の秘密鍵Ｋ０は、本実施の形態では、上述の増幅乱数ビット列発生手段６６に秘密鍵Ｋを与えて出力させた増幅乱数ビット列からＬｋビット分だけ取り出した値を用いている。しかし、これに拘束されるものではなく、例えば、他の手段によって発生させたり、別途にユーザに入力させてもよい。

非線形変換部７０は、α入力１出力の１次無相関な非線形関数ｆ（ｘ）を有しており、乱数ビット列増幅部６０から出力されたα個の増幅乱数ビット列を非線形変換し、Ｎｏビットを有する１個の乱数ビット列を疑似乱数Ｚとして出力するように構成されている。

尚、秘密鍵Ｋは、１２８ビット、２５６ビット、５１２ビット、１０２４ビットの中から選択され、また、選択用乱数ビット列出力手段５１の数α、各選択用乱数ビット列出力手段５１に対応する乱数テーブルの数β、及び選択用乱数ビット列のビット数Ｎｉは、互いにかけ算した値が秘密鍵Ｋのビット数Ｌｋに等しいという条件の範囲内で選択される。

次に、疑似乱数発生方法について第７図に基づき説明する。第７図は、本実施の形態における疑似乱数発生方法の原理を説明するフローチャートである。

まず最初に、乱数ビット列出力部５０は、ユーザからＬｋビットを有する任意の秘密鍵Ｋの入力を受けると（ステップＳ１１）、その秘密鍵Ｋを用いて選択用乱数ビット列出力手段５１の初期値を設定する（ステップＳ１２）。例えば、選択用乱数ビット列出力手段５１が線形フィードバックシフトレジスタによって構成されている場合には、その秘密鍵Ｋに基づいて各シフトレジスタ内に格納される初期値の設定が行われる。

各選択用乱数ビット列出力手段５１の初期値を設定すると、次に、乱数テーブル初期設定手段６５により乱数テーブル部６１の初期設定が行われる（ステップＳ１３）。ここでは、まず、増幅乱数ビット列発生手段６６に秘密鍵Ｋが与えられ、高速で乱数ビット列が発生される。この増幅乱数ビット列発生手段２４により発生された乱数ビット列は、乱数テーブル初期設定手段６５によって、Ｎｏビットごとに分割され、増幅乱数ビット列として各乱数テーブル62_1～$62_{\alpha\beta}$の全ての乱数ビット列格納部Ｒｏに順次格納される。このように、秘密鍵Ｋが与えられることによって、乱数テーブル部６１の初期設定が予め行われる。

上述のステップＳ１１～ステップＳ１３により選択用乱数ビット列出力手段５１と乱数テーブル部６１の初期値の設定が行われると、待機状態となる。そして、平文の暗号化装置（上述の「従来の技術」を参照）への入力をトリガとして、乱数ビット列の増幅処理が開始される（ステップＳ１４～Ｓ１６）。まず最初に、各選択用乱数ビット列出力手段５１によって、それぞれＮｉビットを有する選択用乱数ビット列を乱数テーブルの数であるβ個出力させ、乱数ビット列増幅部６０内に記憶させる（ステップＳ１４）。

それから、乱数テーブル順番入れ替え手段６７により乱数テーブル62_1～$62_{\alpha\beta}$の順番入れ替え処理を行う（ステップＳ１５）。ここでは、まず、入れ替え用乱数発生手段６８によりαβ個の入れ替え用乱数を発生させ、乱数テーブルの順番入れ替え用のテーブル番号として、各乱数テーブル62_1～$62_{\alpha\beta}$に付与する。これらのテーブル番号は、その発生の順番で乱数テーブル62_1から順次付与される。

したがって、各乱数テーブル62_1～$62_{\alpha\beta}$には、１～αβまでのテーブル番号が順不同に付与される。そして、その付与したテーブル番号をもとに乱数テーブル部６１内の増幅乱数ビット列の順番を各乱数テーブル単位で入れ替える処理が行われる。これにより、乱数テーブル部６１の乱数ビット列格納部Ｒｏに格納されている増幅乱数ビット列は、昇順や降順などの予め設定した規則に従って、各乱数テーブル単位で入れ替えられる。

乱数テーブル62_1～$62_{\alpha\beta}$の順番を入れ替える処理が終了すると、増幅乱数ビット列選択手段６４により、各乱数テーブル62_1～$62_{\alpha\beta}$内から該当する増

幅

乱数ビット列を選択する増幅乱数ビット列選択処理が行われる（ステップＳ１６）。増幅乱数ビット列選択手段６４は、ステップＳ１４で乱数ビット列増幅部６０に記憶した各選択用乱数ビット列を用いて、対応する乱数テーブル62_1～$62_{\alpha\beta}$をそれぞれ参照し、各乱数テーブル62_1～$62_{\alpha\beta}$内からそれぞれ該当する増幅乱数ビット列を選択する。

増幅乱数ビット列の選択処理が終了すると、次に、排他的論理和演算処理手段６３により排他的論理和演算処理が行われる（ステップＳ１７）。排他的論理和演算処理手段６３は、各乱数テーブル62_1～$62_{\alpha\beta}$から読み出したαβ個の増幅乱数ビット列を、各選択用乱数ビット列出力手段５１単位で排他的論理和演算処理する。これにより、Ｎｏビットを有するα個の新たな増幅乱数ビット列が生成される。

そして、これらの新たに生成された増幅乱数ビット列は、非線形変換部７０に出力され、非線形変換が行われる（ステップＳ１８）。非線形変換部７０は、予め設定された非線形関数に基づいてＮｏビットのαβ個の増幅乱数ビット列を非線形変換し、Ｎｏビットを有する１個の乱数ビット列を疑似乱数として出力する。

非線形変換部７０から疑似乱数を出力すると、再びステップＳ１４まで戻り、ステップＳ１４からステップＳ１８までの処理を繰り返し行う。そして、平文から暗号文に変換するために必要な分の疑似乱数を発生させる。

上述の疑似乱数発生器２によると、乱数ビット列出力部５０の選択用乱数ビット列出力手段５１によって出力したＮｉビットの選択用乱数ビット列に基づき乱数ビット列増幅部６０の乱数テーブル部６１を参照することで、Ｎｉビットよりも大きなビット数を有するＮｏビットの増幅乱数ビット列を非線形変換部７０に供給することができる。したがって、従来はボトルネックとなっていた非線形変換部７０よりも上流側のスループットを向上させることができ、非線形変換部７０のスループットに近づけることができる。したがって、疑似乱数発生器２全体のスループットを高速化することができる。

また、選択用乱数ビット列出力手段５１からの選択用乱数ビット列の入力に応じて、乱数テーブル順番入れ替え処理を行うので、疑似乱数の暗号強度を増大させることができる。特に、本実施の形態では、乱数テーブル62_1～$62_{\alpha\beta}$の組

合せパターンを（$\alpha\ \beta$）の階乗個（以下、階乗を「！」で表す）にすることができ

る。したがって、乱数テーブル部６１の内容を既知と仮定したときに成立する攻撃では、（２＾（αβ×Ｎｉ））×（αβ）！の計算量が必要となり、この計算量は、Ｌｋビットの秘密鍵を全数探索する場合の計算量よりも多くなることから、十分な暗号強度を備えていることがわかる。

また、上述の疑似乱数発生器２は、一の選択用乱数ビット列出力手段５１から出力した乱数ビット列を用いて複数（β個）の乱数テーブルを参照し、各乱数テーブルから選択した乱数ビット列に排他的論理和演算を施す処理を行っている。したがって、乱数テーブル部６１から読み出した増幅乱数ビット列をそのまま非線形変換部７０に出力した場合のように暗号強度が増幅乱数ビット列発生手段６６そのものに依存するのを防ぎ、暗号強度を更に向上させている。

次に、本実施の形態における具体的な一実施例について説明する。第８図は、本実施例の疑似乱数発生器２を概略的に示す概念図、第９図は、乱数テーブル部６１を概略的に示す概念図である。尚、本実施例では、各設定値（パラメータ）を以下のように設定した場合を例に説明する。

選択用乱数ビット列出力手段の数：８個（α＝８）

各選択用乱数ビット列出力手段に対応した乱数テーブルの数：２個（β＝２）

乱数テーブルのインデックス部の長さ：２＾８個（Ｎｉ＝８）

乱数テーブルの乱数ビット列部の長さ：２＾１６個（Ｎｏ＝１６）

秘密鍵の長さ：１２８ビット（Ｌｋ＝１２８）

非線形変換部７０の非線形関数ｆ（ｘ）：

f(x) = x1 + x5
+ x1x2 + x1x3 + x2x3 + x2x5 + x2x6 + x3x6
+ x1x7 + x2x7 + x4x8 + x5x8
+ x1x2x3 + x1x2x4 + x1x3x4 + x2x3x4 + x1x2x5
+ x2x4x5 + x3x4x5 + x1x2x6 + x2x3x6 + x1x4x6
+ x4x5x6 + x1x2x7 + x2x3x7 + x1x4x7 + x1x5x7
+ x2x5x7 + x4x5x7 + x1x6x7 + x4x6x7 + x5x6x7
+ x1x2x8 + x1x3x8 + x2x3x8 + x3x4x8 + x1x5x8
+ x3x5x8 + x4x5x8 + x3x6x8 + x4x6x8 + x5x6x8

+ x1x7x8 + x2x7x8
+ x1x2x4x5 + x1x3x4x5 + x2x3x4x5 + x1x2x4x6
+ x1x3x4x6 + x2x3x4x6 + x1x4x5x6 + x2x4x5x6
+ x3x4x5x6 + x1x2x3x7 + x1x2x4x7 + x2x3x4x7
+ x1x2x5x7 + x1x4x5x7 + x2x4x5x7 + x1x2x6x7
+ x1x3x6x7 + x2x3x6x7 + x1x4x6x7 + x2x4x6x7
+ x3x4x6x7 + x1x5x6x7 + x2x5x6x7 + x3x5x6x7
+ x1x2x4x8 + x1x2x5x8 + x1x3x5x8 + x1x4x5x8
+ x1x2x6x8 + x2x3x6x8 + x1x4x6x8 + x2x5x6x8
+ x3x5x6x8 + x1x3x7x8 + x1x4x7x8 + x2x4x7x8
+ x3x4x7x8 + x2x5x7x8
+ x1x2x3x4x5 + x1x2x3x4x6 + x1x3x4x5x6
+ x2x3x4x5x6 + x1x2x4x5x7 + x2x3x4x5x7
+ x1x2x4x6x7 + x1x3x4x6x7 + x1x4x5x6x7
+ x2x4x5x6x7 + x1x2x3x4x8 + x1x2x3x5x8
+ x1x2x4x5x8 + x1x2x3x6x8 + x1x2x4x6x8
+ x1x3x4x6x8 + x2x3x5x6x8 + x1x4x5x6x8
+ x2x4x5x6x8 + x1x2x3x7x8 + x1x3x4x7x8
+ x1x3x5x7x8 + x2x3x5x7x8 + x3x4x5x7x8
+ x1x3x6x7x8 + x3x4x6x7x8
+ x1x2x3x4x5x8 + x1x2x3x4x6x8
+ x1x3x4x5x6x8 + x2x3x4x5x6x8
+ x1x2x3x4x7x8 + x1x2x3x5x7x8
+ x1x2x4x5x7x8 + x1x3x4x5x7x8
+ x1x3x4x6x7x8 + x2x3x4x6x7x8
+ x1x2x5x6x7x8 + x1x3x5x6x7x8

本実施例では、各選択用乱数ビット列出力手段５１が、ユーザから与えられる秘密鍵Ｋに基づいて線形フィードバックシフトレジスタ５３の再構成を行い、その再構成後の線形フィードバックシフトレジスタ５３を用いて選択用乱数ビッ

ト列を出力するように構成されている。

まず最初に、この選択用乱数ビット列出力手段５１の構成及びその動作について説明する。選択用乱数ビット列出力手段５１は、第８図に示すように、初期値設定手段５２、線形フィードバックシフトレジスタ５３、線形フィードバックシフトレジスタ再構成手段５４を有している。

初期値設定手段５２は、ユーザから与えられる秘密鍵Ｋに基づいて初期値を設定するものであり、秘密鍵Ｋをビット列に変換し、初期値として線形フィードバックシフトレジスタ５３のシフトレジスタ内に割り当てるように構成されている。初期値設定手段５２は、本実施例では、ＲＣ４　Ｓｙｐｐｅｔｒｉｃ　Ｓｔｒｅａｐ　Ｃｉｐｈｅｒ（ＲＳＡ　Ｄａｔａ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃ．製）を用いており、増幅乱数ビット列発生手段６６と共用している。

線形フィードバックシフトレジスタ５３は、上述の「従来の技術」で説明したものと同様に、１ビットの情報を記憶できるｎ個のシフトレジスタと、排他的論理和演算回路を有している。そして、本実施の形態では、１周期分のビット数ｍが（２＾ｎ）－１個となるビット列、いわゆるＭ系列を出力可能な構成に予め設定されている。

第１１図は、本実施の形態における線形フィードバックシフトレジスタ５３の初期多項式を例示するものである。初期多項式は、Ｍ系列を出力するように予め設定されている特性多項式であり、１項目の指数部分がシフトレジスタの個数を示し、２項目以降の指数部分が排他的論理和演算回路に接続された結線位置を示している。例えば、１段目の線形フィードバックシフトレジスタ（ＬＦＳＲ１）５３は、１２９個のシフトレジスタを有し、８０番目、８番目、１番目のシフトレジスタがフィードバックタップによって排他的論理和演算回路に接続されていることを示している。尚、本実施の形態では、シフトレジスタの個数ｎは、全て素数個に設定されている。

線形フィードバックシフトレジスタ再構成手段５４は、線形フィードバックシフトレジスタ５３の構成を秘密鍵Ｋによって動的に変更して再構成するものである。具体的には、出力系列がＭ系列のビット列をｓ個ごとにサンプルした新ビット列は、Ｍ系列の１周期分のビット数ｍ（＝（２＾ｎ）－１）と導出値ｓとが互

いに素であるとき、すなわち、１以外の共通の約数を持たないときは、他の構成

を有する線形フィードバックシフトレジスタのM系列になり、また、バーレイキャンプマッセイアルゴリズムによって、少なくとも２周期分以上のビット数を有するビット列から、そのビット列を出力可能な等価で最小の線形フィードバックシフトレジスタの特性多項式を求めることができることを利用して、線形フィードバックシフトレジスタ５３の再構成を行う。

線形フィードバックシフトレジスタ再構成手段５４は、初期値設定手段５２によって与えられた初期値から導出値ｓを算出し、導出値ｓと線形フィードバックシフトレジスタ５３の１周期分のビット数ｍ（＝（２＾ｎ）－１）を２倍した値２ｍとを乗算し、線形フィードバックシフトレジスタ５３から出力させるビット列のビット数２ｍｓを算出する。

そして、初期値をもとに線形フィードバックシフトレジスタ５３から２ｍｓ個のビット列を出力させ、その２ｍｓ個のビット列から導出値ｓの間隔ごとにビット列を取り出して新ビット列を生成し、その新ビット列を用いてバーレイキャンプマッセイアルゴリズムにより線形フィードバックシフトレジスタ５３の構成を変更する。

尚、線形フィードバックシフトレジスタ５３から出力させるビット列のビット数は、新ビット列のビット数が２ｍ個以上であれば、等価な最小の線形フィードバックシフトレジスタを求めることができるので、２ｍｓ個以上であればよい。

バーレイキャンプマッセイアルゴリズムとは、線形フィードバックシフトレジスタ５３のシフトレジスタの個数ｎ（線形複雑度）の２倍以上のビット数を有するビット列を入手することで、そのビット列を出力可能な等価な最小の線形フィードバックシフトレジスタを得ることができるというアルゴリズムである。バーレイキャンプマッセイアルゴリズムについては、例えば、文献１「暗号理論入門（第２版）」、共立出版社、岡本栄司著、２００２年４月１０日発行、に詳細に説明されている。

第１２図は、線形フィードバックシフトレジスタ５３の再構成処理を説明するフローチャートである。

まず最初に、初期値設定手段５２によって初期値が設定される（ステップＳ４１）。初期値は、利用者から与えられるＬｋビットの秘密鍵Ｋに基づいて設定さ

れる。初期値設定手段５２において秘密鍵Ｋから初期値が

ードバックシフトレジスタ５３を求めることができるので、２m個のビット数を有する新ビット列から新たな線形フィードバックシフトレジスタ５３の特性多項式を導出して、再構成を行う。

再構成後の線形フィードバックシフトレジスタ５３は、再構成前と同一の次数及び異なる結線の特性多項式を有し、同一の初期値を与えた場合に、再構成前と異なるM系列を出力可能な構成を有する。

線形フィードバックシフトレジスタ再構成手段１４による線形フィードバックシフトレジスタ５３の再構成が終了すると、再構成された線形フィードバックシフトレジスタ５３から初期値をもとに選択用乱数ビット列を発生させる処理が行われる（ステップＳ４７）。これにより、乱数ビット列出力部５０からは再構成前とは異なるM系列の選択用乱数ビット列が出力される。

尚、上記のステップＳ４６で、新ビット列に基づいて線形フィードバックシフトレジスタ５３の構成を再構成する代わりに、新ビット列を出力可能な構成を有する第２の線形フィードバックシフトレジスタを生成し、ステップＳ４７で、その第２の線形フィードバックシフトレジスタによって初期値をもとに乱数ビット列を発生させてもよい。これによれば、線形フィードバックシフトレジスタ５３を２つに分けることができ、より秘匿性の向上を図ることができる。

上記の選択用乱数ビット列出力手段５１は、線形フィードバックシフトレジスタ５３の構成を初期値に基づいて容易かつ動的に変更することができ、変更後もM系列を出力させることができる。したがって、攻撃者は、再構成前の線形フィードバックシフトレジスタ５３の構成を取得することができない。これにより、従来、線形フィードバックシフトレジスタ５３の構成が既知であることを前提に成り立っていた既存の暗号解読法は、成立しなくなる。したがって、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

次に、上記の選択用乱数ビット列出力手段５１を備えた疑似乱数発生器２による疑似乱数発生方法について説明する。第１０図は、本実施例における疑似乱数発生方法を説明するフローチャートである。

まず最初に、乱数ビット列出力部５０は、ユーザから１２８ビット（Ｌｋ＝１２８）を有する任意の秘密鍵Ｋの入力を受け取ると、その秘密鍵Ｋに基づいて再

構成前の線形フィードバックシフトレジスタ５３の初期値を設定する（ステップＳ２１）。

そして、その初期値に基づいて線形フィードバックシフトレジスタ５３を再構成し（ステップＳ２２）、再構成後の線形フィードバックシフトレジスタ５３に初期値を設定する（ステップＳ２３）。この初期値の設定を、全ての乱数ビット列出力手段11_1～11_8について行う。

次に、乱数ビット列増幅部６０は、乱数テーブル部６１の初期設定を行う（ステップＳ２４）。ここでは、まず、増幅乱数ビット列発生手段６６に秘密鍵Ｋを与え、高速で乱数ビット列を発生させる処理が行われるが、本実施例では、上述のように、増幅乱数ビット列発生手段６６と選択用乱数ビット列出力手段51_1～$_8$の初期値設定手段５２とを共用しているので、別途出力することはせずに、線形フィードバックシフトレジスタ５３の初期値として出力した乱数ビット列をそのまま用いる。

乱数テーブル初期設定手段６５は、その乱数ビット列を１６ビット（Ｎｏ＝１６）ごとに分割し、増幅乱数ビット列として各乱数テーブル62_1～62_{16}の全ての乱数ビット列格納部Ｒｏに順次格納する。

以上の初期値設定段階が終了すると（ステップＳ２１～Ｓ２４）、待機状態となる。そして、平文の暗号化装置（従来技術を参照）への入力をトリガとして、疑似乱数を発生させる処理（ステップＳ２５～Ｓ２７）に移行する。

ここでは、各選択用乱数ビット列出力手段51_1～51_8ごとにそれぞれ選択用乱数ビット列を出力させ、乱数ビット列増幅部６０のバッファ内にそれぞれ記憶させる処理が行われる。具体的には、各選択用乱数ビット列出力手段51_1～51_8から８ビットの選択用乱数ビット列がそれぞれ出力され（ステップＳ２７）、その数が各選択用乱数ビット列出力手段１に対して２個分（$\beta=2$）であり（ステップＳ２６でＹｅｓ）、各選択用乱数ビット列出力手段51_1～51_8にそれぞれ対応する分である場合（ステップＳ２５でＹｅｓ）には、必要数の選択乱数ビット列が得られたとして次の乱数ビット列増幅段階に移行する。したがって、ここまでの処理により、バッファ内には８ビットを有する１６個の選択用乱数ビット列が記憶される。

次に、秘密鍵Ｋ０に基づき入れ替え用乱数発生手段６８により１６個の入れ替え用乱数を発生させ（ステップＳ２８）、乱数テーブルの順番入れ替え処理が行われる（ステップＳ２９）。ここでは、１６個の乱数が順番入れ替え用のテーブル番号として、乱数テーブル62_1～62_{16}に付与される。したがって、１番～１６番までのテーブル番号が順不同で乱数テーブル62_1～62_{16}に付与される。そして、その付与されたテーブル番号をもとに各乱数テーブル62_1～62_{16}の順番の入れ替えを行う。ここでは、選択用乱数ビット列出力手段51_1～51_nに対してテーブル番号が１番～１６番に順番に並ぶように降順に入れ替える処理が行われる。これにより、乱数テーブル部６１内の増幅乱数ビット列は、その順番が乱数テーブル単位でランダムに入れ替えられる。

そして次に、各乱数テーブル62_1～62_{16}内から該当する増幅乱数ビット列を選択する処理が行われる（ステップＳ３０～Ｓ３２）。例えば、選択用乱数ビット列11_1から出力されバッファに記憶された１番目の選択用乱数ビット列を引数として乱数テーブル62_1が参照される（ステップＳ３２）。そして、その引数と等しい値を有するインデックス番号を選択し、そのインデックス番号に対応する乱数ビット列格納部Ｒｏに格納された増幅乱数ビット列を選択する。

例えば、選択用乱数ビット列出力手段51_1から出力され乱数テーブル62_1に対応するものとしてバッファに記憶された選択用乱数ビット列が「００００００１１」である場合、これを８桁の２進数とみなし、１０進数に変換して引数「３」を得る。この引数「３」を用いて乱数テーブル62_1を参照し、インデックス部Ｒｏのインデックス番号が「３」の乱数ビット列格納部Ｒｏに格納されている増幅乱数ビット列「０１０１１０１０１１０１１１０１１０」を選択する。

そして、乱数テーブル62_1と乱数テーブル62_2からそれぞれ増幅乱数ビット列を選択すると（ステップＳ３１でＹｅｓ）、これら２つの増幅乱数ビット列の排他的論理和演算処理を行い（ステップＳ３３）、１６ビットを有する１個の新たな増幅乱数ビット列を生成する。

そして、同様の処理を各乱数テーブル62_3～62_{16}について行い（ステップＳ３０でＹｅｓ）、合計で８個の新たな増幅乱数ビット列を生成すると、非線形変換部７０に出力して、非線形変換段階に移行する。

非線形変換部７０では、乱数ビット列増幅部６０よりこれらのＮｏビットを有する８個の増幅乱数ビット列を入力すると、非線形関数ｆ（ｘ）により非線形変換し（ステップＳ３４）、１６ビットを有する１個の乱数ビット列を得る。そして、上記ステップＳ２５～ステップＳ３４の処理を繰り返し実行して必要数の疑似乱数を得る。

本実施例については、処理速度の高速化及び乱数性が適切に確保されているかについて実験を行っており、その結果、従来と比較して１７０倍も処理速度を向上でき、同時に適切な乱数性も確保されているとの結果を得た。以下に、その実験内容及び実験結果について説明する。

実験に使用したコンピュータは、ＣＰＵ：Ｐｅｎｔｉｕｍ（登録商標）４（１．７ＧＨｚ）、メモリ：２５６ＭＢである。また、各設定値は、上述の実施例と同一のものとする。そして、入れ替え用乱数ビット列発生手段２８に用いられる秘密鍵Ｋ０は、１６進数表記で以下のものに固定した状態として実験を行った。

$K0 = (f1e2d3c4b5a69788796a5b4c3d2e1f10)_{16}$

第1.３図は、スループットの計測結果を示す表である。表中の従来型とは、８個の線形フィードバックシフトレジスタ５３と、非線形変換部７０を用いて構成した、第１７図に示すような従来の非線形コンバイナ型疑似乱数発生器を示す。

本実験結果によれば、第１３図に示すように、疑似乱数発生器２の平均スループットが、線形フィードバックシフトレジスタ５３そのものの平均スループットから、非線形変換部７０の平均スループットに向上しており、更に、従来型の約１７０倍（116.4Mbps/sec÷0.680Mbps/sec=171.176…）になっていることがわかる。したがって、このスループット計測結果から、乱数テーブル６２を用いたことが疑似乱数発生器２の高速化に有効であることがわかる。

本実施例における疑似乱数発生器２のスループットは、次式（１）で表される。

【数式】

$$\frac{1}{T}=\frac{N_I}{N_O}\left(\frac{n}{T_1}+\frac{1}{T_2}+\frac{1}{T_3}\right)+\frac{nm}{T_4}+\frac{1}{T_5} \quad (1)$$

Ｔ１は、１つの線形フィードバックシフトレジスタ５３の平均スループットを示し、Ｔ２は、ＲＣ４（増幅乱数ビット列発生手段６６）の平均スループットを

示す。また、Ｔ３は、乱数テーブル順番入れ替え手段６７による乱数テーブル入れ替え処理の平均スループットを示し、Ｔ４は、１つの乱数テーブル６２の平均スループットを示す。そして、Ｔ５は、非線形変換部７０の平均スループットを示す。上記式（１）から乱数テーブル６２の計算量が無視できると仮定すると、Ｎｏビット／Ｎｉビットを小さくするほど非線形変換部７０のスループットに近づけることができ、高速化を図ることができる。

疑似乱数の暗号強度の検証については、ＮＩＳＴという疑似乱数検定ツールを用いて検定を行った。ＮＩＳＴとは、物理乱数及び疑似乱数生成器からの出力データについて乱数性のテストを行うツールであり、１６項目からのテストからなる統計のパッケージである。ＮＩＳＴについては、http://crsc.nist.gov/rug.に詳しく説明されている。第１４図は、本検定に使用したＮＩＳＴのパラメータを示す表である。各種テストを行うことによって出力されたp-valueが０＜p-value＜１を満たす場合に、そのテスト項目をパスしたとみなしている。本実施例による疑似乱数発生器２の疑似乱数を検定したところ、全てのテスト項目をパスしていることが確認できた。第１５図は、今回の実験によるＮＩＳＴの検定結果を示す図である。

尚、上述の実施例に示した各設定値は、暗号の安全性を確認するために設定したものであり、これに限定されるものではない。また、本発明は、上述の実施の形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々の変更、組み合わせが可能である。

［発明の効果］

以上説明したように、本発明に係る疑似乱数発生方法によれば、出力系列がM系列のビット列をｓ個ごとにサンプルしたビット列は、そのM系列の１周期分のビット数ｍ（＝（２＾ｎ）－１）と導出値ｓが互いに素であるときには、他の構成を有する線形フィードバックシフトレジスタのM系列を構成し、また、バーレイキャンプマッセイアルゴリズムによって、少なくとも２周期分以上のビット数を有するビット列から線形フィードバックシフトレジスタを求めることができることを利用して、線形フィードバックシフトレジスタの構成を初期値に基づいて動的に変更することができ、変更後の線形フィードバックシフトレジスタからM

系列のビット列を出力させることができる。

したがって、解読者は、疑似乱数発生器から出力される疑似乱数に基づいて再構成前の線形フィードバックシフトレジスタの構成を得ることができず、初期値や秘密鍵も解読することができない。この結果、高い暗号強度を得ることができ、情報の秘匿性を保つことができる。

また、他の発明によれば、秘密鍵に基づいて所定のビット数を有する選択用乱数ビット列を出力させ、その選択用乱数ビット列を用いて乱数テーブルを参照することにより、乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択し、非線形変換手段によって非線形変換して疑似乱数として出力させるので、小さなビット列を有する選択用乱数ビット列に基づいて、より大きなビット数を有する増幅乱数ビット列を得ることができる。

したがって、非線形変換手段に入力される乱数ビット列をより大きなビット数を有するものにすることができる。これにより、従来、ボトルネックとなっていた非線形変換手段よりも上流側の乱数ビット列を出力する部分のスループットを向上させ、非線形変換手段のスループットに近づけることができ、疑似乱数発生器全体のスループットを高速化することができる。

[図面の簡単な説明]

[第１図]

本実施の形態における疑似乱数発生器を説明する図である。

[第２図]

本実施の形態における線形フィードバックシフトレジスタの初期多項式を例示するものである。

[第３図]

本実施の形態における疑似乱数発生器の動作を説明するフローチャートである。

[第４図]

疑似乱数発生器の原理を示す説明図である。

[第５図]

乱数テーブル部の説明図である。

[第６図]

乱数ビット列増幅部内に構成される各構成要素を説明する原理図である。

[第７図]

本実施の形態における疑似乱数発生方法を説明するフローチャートである。

[第８図]

本実施例における疑似乱数発生器を概略的に示す概念図である。

[第９図]

乱数テーブル部を概略的に示す概念図である。

[第１０図]

本実施例における疑似乱数発生方法を説明するフローチャートである。

[第１１図]

本実施の形態における線形フィードバックシフトレジスタの初期多項式を例示するものである。

[第１２図]

線形フィードバックシフトレジスタの再構成処理を説明するフローチャートである。

[第１３図]

スループットの計測結果を示す表である。

[第１４図]

本検定に使用したＮＩＳＴのパラメータを示す表である。

[第１５図]

ＮＩＳＴの検定結果を示す図である。

[第１６図]

従来の逐次暗号方式を説明する図である。

[第１７図]

暗号化装置の疑似乱数発生器を説明する図である。

[第１８図]

一般的な線形フィードバックシフトレジスタの構成を簡単に説明する図である。

[符号の説明]

1　疑似乱数発生器（第１の実施の形態）

２　疑似乱数発生器（第２の実施の形態）

１０　疑似乱数生成部

１１　線形フィードバックシフトレジスタ

１２　線形フィードバックシフトレジスタ再構成手段

２０　非線形変換部

５０　乱数ビット列出力部

５１　選択用乱数ビット列出力手段

５２　初期値設定手段

５３　線形フィードバックシフトレジスタ

５４　線形フィードバックシフトレジスタ再構成手段

６０　乱数ビット列増幅部

６１　乱数テーブル部

62_1～$62_{\alpha\beta}$　乱数テーブル

６３　排他的論理和演算処理手段

６４　増幅乱数ビット列選択手段

６５　乱数テーブル初期設定手段

６６　増幅乱数ビット列発生手段

６７　乱数テーブル順番入れ替え手段

６８　入れ替え用乱数発生手段

７０　非線形変換部

請求の範囲

1．　（補正後）ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタの初期値を設定する第１ステップと、

所定の演算処理により前記初期値から前記線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める第２ステップと、

該導出値と前記線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値とを乗算して、前記線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出する第３ステップと、

前記算出したビット数分のビット列を前記線形フィードバックシフトレジスタから前記初期値をもとに出力させる第４ステップと、

該出力したビット列から前記導出値の間隔ごとにビット列を取り出して新ビット列を生成する第５ステップと、

該新ビット列を出力可能な構成に前記線形フィードバックシフトレジスタの構成を再構成する第６ステップと、

該再構成した後の線形フィードバックシフトレジスタから前記初期値をもとに疑似乱数を発生させる第７ステップと、

を有することを特徴とする疑似乱数発生方法。

2．　前記初期値に対してハッシュ関数を施してハッシュ値を求め、該ハッシュ値に最も近似した素数を導出値として採用することを特徴とする請求項１に記載の疑似乱数発生方法。

3．　前記線形フィードバックシフトレジスタの再構成は、バーレイキャンプマッセイアルゴリズムを用いて行われることを特徴とする請求項１または２に記載の疑似乱数発生方法。

4．　前記第７ステップで発生させた疑似乱数を非線形変換する第８ステップ

を有することを特徴とする請求項１～３のいずれかに記載の疑似乱数発生方法。

５．　（補正後）ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタと、

秘密鍵に基づき前記線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、

所定の演算処理により前記初期値から前記線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める導出値算出手段と、

前記線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値と前記導出値とを乗算して、前記線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、

該ビット数算出手段により算出したビット数分のビット列を前記線形フィードバックシフトレジスタから前記初期値をもとに出力させるビット列出力手段と、

該出力したビット列から前記導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、

該新ビット列を出力可能な構成に前記線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、

該再構成後の線形フィードバックシフトレジスタから前記初期値をもとに疑似乱数を発生させる疑似乱数発生手段と、を有することを特徴とする疑似乱数発生器。

６．　前記線形フィードバックシフトレジスタ再構成手段の代わりに、新ビット列を出力可能な構成を有する第２の線形フィードバックシフトレジスタを生成する線形フィードバックシフトレジスタ生成手段を設け、

前記疑似乱数発生手段は、前記第２の線形フィードバックシフトレジスタによって初期値をもとに疑似乱数を発生させることを特徴とする請求項５に記載の疑似乱数発生器。

７．　（補正後）秘密鍵に基づいて所定のビット数を有する選択用乱数ビット

列を出力する

乱数ビット列出力部と、該乱数ビット列出力部から出力された選択用乱数ビット列に基づいて前記選択用乱数ビット列のビット数よりも大きなビット数を有する増幅乱数ビット列を出力する乱数ビット列増幅部と、該乱数ビット列増幅部から出力された増幅乱数ビット列を非線形変換して疑似乱数を出力する非線形変換部とを有し、

前記乱数ビット列出力部は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタと、秘密鍵に基づき前記線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、所定の演算処理により前記初期値から前記線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める導出値算出手段と、前記線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値と前記導出値とを乗算して、前記線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、該ビット数算出手段により算出したビット数分のビット列を前記線形フィードバックシフトレジスタから前記初期値をもとに出力させるビット列出力手段と、該ビット列出力手段から出力したビット列から前記導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、該新ビット列を出力可能な構成に前記線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、該線形フィードバックシフトレジスタ再構成手段によって再構成された再構成後の線形フィードバックシフトレジスタを用いて前記初期値をもとに前記選択用乱数ビット列を出力する選択用乱数ビット列出力手段とを有し、

前記乱数ビット列増幅部は、前記選択用乱数ビット列よりも大きなビット数を有する増幅乱数ビット列を予め複数格納した乱数テーブルと、前記選択用乱数ビット列出力手段から出力された選択用乱数ビット列を用いて前記乱数テーブルを参照することにより、前記乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択可能な増幅乱数ビット列選択手段とを有し、

非線形変換部は、該増幅乱数ビット列選択手段により選択された増幅乱数ビット列を非線形関数によって非線形変換し疑似乱数として出力する非線形変換手段

とを有することを特徴とする疑似乱数発生器。

8． （補正後）前記乱数ビット列増幅部は、

前記秘密鍵が与えられることにより前記秘密鍵に基づいて前記増幅乱数ビット列を発生させる増幅乱数ビット列発生手段と、

該増幅乱数ビット列発生手段により発生させた増幅乱数ビット列を前記乱数テーブルに格納して、前記乱数テーブルの初期設定を行う乱数テーブル初期設定手段を有することを特徴とする請求項７に記載の疑似乱数発生器。

9． （補正後）前記乱数ビット列出力部は、前記選択用乱数ビット列出力手段が複数設けられ、

前記乱数ビット列増幅部は、前記乱数テーブルが前記各選択用乱数ビット列出力手段にそれぞれ対応するように設けられ、前記増幅乱数ビット列選択手段が前記各選択用乱数ビット列出力手段から各々出力された前記各選択用乱数ビット列を用いて前記各選択用乱数ビット列出力手段ごとに対応する前記乱数テーブルをそれぞれ参照し、前記各乱数テーブル内からそれぞれ該当する増幅乱数ビット列を選択し、

前記非線形変換部は、前記非線形変換手段が前記各増幅乱数ビット列選択手段によって前記各乱数テーブルから選択された前記各増幅乱数ビット列を用いて非線形関数により非線形変換し疑似乱数として出力することを特徴とする請求項７または８に記載の疑似乱数発生器。

１０． （補正後）前記乱数ビット列増幅部は、前記各選択用乱数ビット列出力手段ごとにそれぞれ複数の乱数テーブ

ルを設け、

前記増幅乱数ビット列選択手段により前記各乱数テーブル内から選択された各増幅乱数ビット列を前記乱数ビット列出力部の前記選択用乱数ビット列出力手段ごとに排他的論理和演算して前記非線形変換部の前記非線形変換手段に出力する排他的論理和演算処理手段を有することを特徴とする請求項９に記載の疑似乱数発生器。

１１．　（補正後）前記乱数ビット列増幅部は、所定のタイミングで前記各乱数テーブル同士の入れ替えを行う乱数テーブル入れ替え手段を有することを特徴とする請求項９または１０に記載の疑似乱数発生器。

１２．　（補正後）前記乱数テーブル入れ替え手段は、

前記各乱数テーブルを参照するために必要な選択用乱数ビット列を前記乱数ビット列出力部の前記選択用乱数ビット列出力手段が出力するごとに、前記各乱数テーブル同士の入れ替えを行うことを特徴とする請求項１１に記載の疑似乱数発生器。

１３．　前記乱数テーブル入れ替え手段は、

前記各乱数テーブルの個数と等しい個数の乱数テーブル入れ替え用乱数を発生させ、

該乱数テーブル入れ替え用乱数を前記乱数テーブルのテーブル番号として各乱数テーブルに付与し、前記テーブル番号をもとに予め設定された規則に従って前記乱数テーブルの順番を入れ替えることを特徴とする請求項１１または１２に記載の疑似乱数発生器。

１４．（補正後）コンピュータを、

秘密鍵に基づいて所定のビット数を有する選択用乱数ビット列を出力する乱数ビット列出力部と、該乱数ビット列出力部から出力された選択用乱数ビット列に基づいて前記選択用乱数ビット列のビット数よりも大きなビット数を有する増幅

乱数ビット列を出力する乱数ビット列増幅部と、該乱数ビット列増幅部から出力された増幅乱数ビット列を非線形変換して疑似乱数を出力する非線形変換部として機能させるための疑似乱数発生プログラムであって、

前記乱数ビット列出力部は、ｎ個のシフトレジスタを有し、１周期分のビット数が（２＾ｎ）－１個となるビット列を出力可能な線形フィードバックシフトレジスタと、秘密鍵に基づき前記線形フィードバックシフトレジスタの初期値を設定する初期値設定手段と、所定の演算処理により前記初期値から前記線形フィードバックシフトレジスタの１周期分のビット数と互いに素である導出値を求める導出値算出手段と、前記線形フィードバックシフトレジスタの１周期分のビット数を２倍以上した値と前記導出値とを乗算して、前記線形フィードバックシフトレジスタにより出力させるビット列のビット数を算出するビット数算出手段と、該ビット数算出手段により算出したビット数分のビット列を前記線形フィードバックシフトレジスタから前記初期値をもとに出力させるビット列出力手段と、該ビット列出力手段から出力したビット列から前記導出値の間隔ごとにビット列を取り出して新ビット列を生成する新ビット列生成手段と、該新ビット列を出力可能な構成に前記線形フィードバックシフトレジスタの構成を再構成する線形フィードバックシフトレジスタ再構成手段と、該線形フィードバックシフトレジスタ再構成手段によって再構成された再構成後の線形フィードバックシフトレジスタを用いて前記選択用乱数ビット列を出力する選択用乱数ビット列出力手段とを有し、

前記乱数ビット列増幅部は、前記選択用乱数ビット列よりも大きなビット数を有する増幅乱数ビット列を予め複数格納した乱数テーブルと、前記選択用乱数ビット列出力手段から出力された選択用乱数ビット列を用いて前記乱数テーブルを参照することにより、前記乱数テーブル内の複数の増幅乱数ビット列の中から該当する増幅乱数ビット列を選択可能な増幅乱数ビット列選択手段とを有し、

前記非線形変換部は、前記増幅乱数ビット列選択手段により選択された増幅乱数ビット列を非線形関数によって非線形変換し疑似乱数として出力する非線形変換手段を有することを特徴とする疑似乱数発生プログラム。

１５．　（補正後）前記乱数ビット列増幅部は、前記秘密鍵が与えられることにより前記秘密鍵に基づいて前記増幅乱数ビット列を発生させ、前記乱数テーブルに格納して、前記乱数テーブルの初期設定を行う乱数テーブル初期設定手段としてコンピュータを機能させることを特徴とする請求項１４に記載の疑似乱数発生プログラム。

１６．　（補正後）前記乱数ビット列出力部は、前記選択用乱数ビット列出力手段が複数設けられ、

前記乱数ビット列増幅部は、前記乱数テーブルが前記各選択用乱数ビット列出力手段にそれぞれ対応するように設けられ、

前記増幅乱数ビット列選択手段が前記各選択用乱数ビット列出力手段から各々出力された前記各選択用乱数ビット列を用いて前記各選択用乱数ビット列出力手段ごとに対応する前記乱数テーブルをそれぞれ参照し、前記各乱数テーブル内からそれぞれ該当する増幅乱数ビット列を選択し、

前記非線形変換部は、前記非線形変換手段が前記各増幅乱数ビット列選択手段によって前記各乱数テーブルから選択された前記各増幅乱数ビット列を用いて非線形関数により非線形変換し疑似乱数として出力することを特徴とする請求項１４または１５に記載の疑似乱数発生プログラム。

１７．　（補正後）前記乱数ビット列増幅部は、前記各選択用乱数ビット列出力手段ごとにそれぞれ複数の乱数テーブルを設け、

前記増幅乱数ビット列選択手段により前記各乱数テーブル内から選択された各増幅乱数ビット列を前記乱数ビット列出力部の前記選択用乱数ビット列出力手段ごとに排他的論理和演算して前記非線形変換部の前記非線形変換手段に出力する排他的論理和演算処理手段としてコンピュータを機

能させることを特徴とする請求項１６に記載の疑似乱数発生プログラム。

１８．　（補正後）前記乱数ビット列増幅部は、所定のタイミングで前記各乱数テーブル同士の入れ替えを行う乱数テーブル入れ替え手段としてコンピュータを機能させることを特徴とする請求項１６または１７に記載の疑似乱数発生プログラム。

１９．　（補正後）前記乱数テーブル入れ替え手段は、

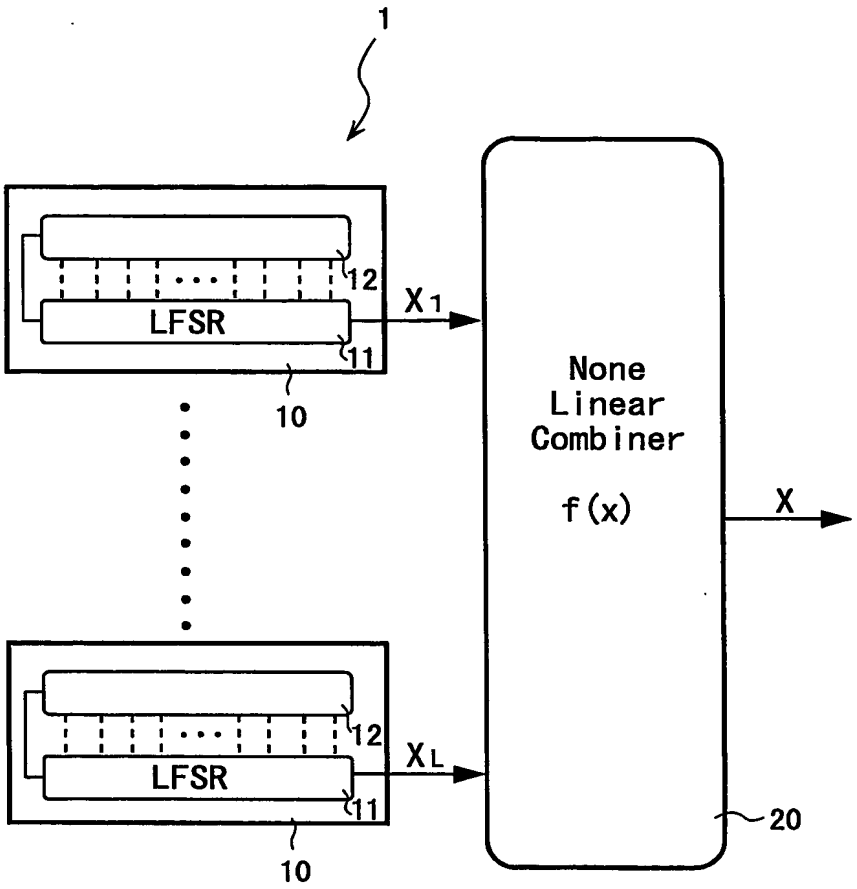
前記各乱数テーブルを参照するために必要な選択用乱数ビット列を前記乱数ビット列出力部の前記選択用乱数ビット列出力手段が出力するごとに、前記各乱数テーブル同士の入れ替えを行うことを特徴とする請求項１８に記載の疑似乱数発生プログラム。

２０．　前記乱数テーブル入れ替え手段は、

前記各乱数テーブルの個数と等しい個数の乱数テーブル入れ替え用乱数を発生させ、

該乱数テーブル入れ替え用乱数を前記乱数テーブルのテーブル番号として各乱数テーブルに付与し、前記テーブル番号をもとに予め設定された規則に従って前記乱数テーブルの順番を入れ替えることを特徴とする請求項１８または１９に記載の疑似乱数発生プログラム。

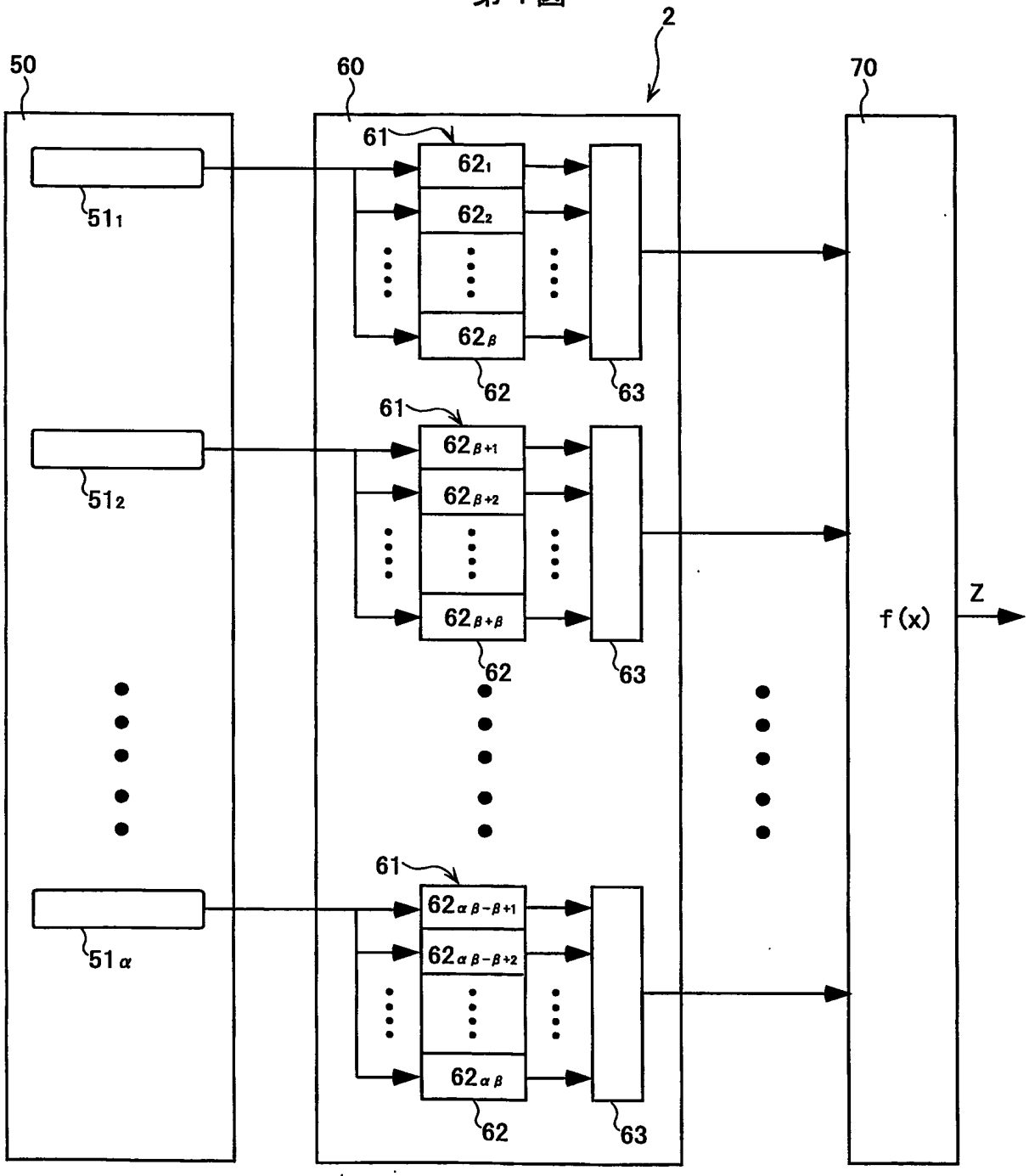
第１図



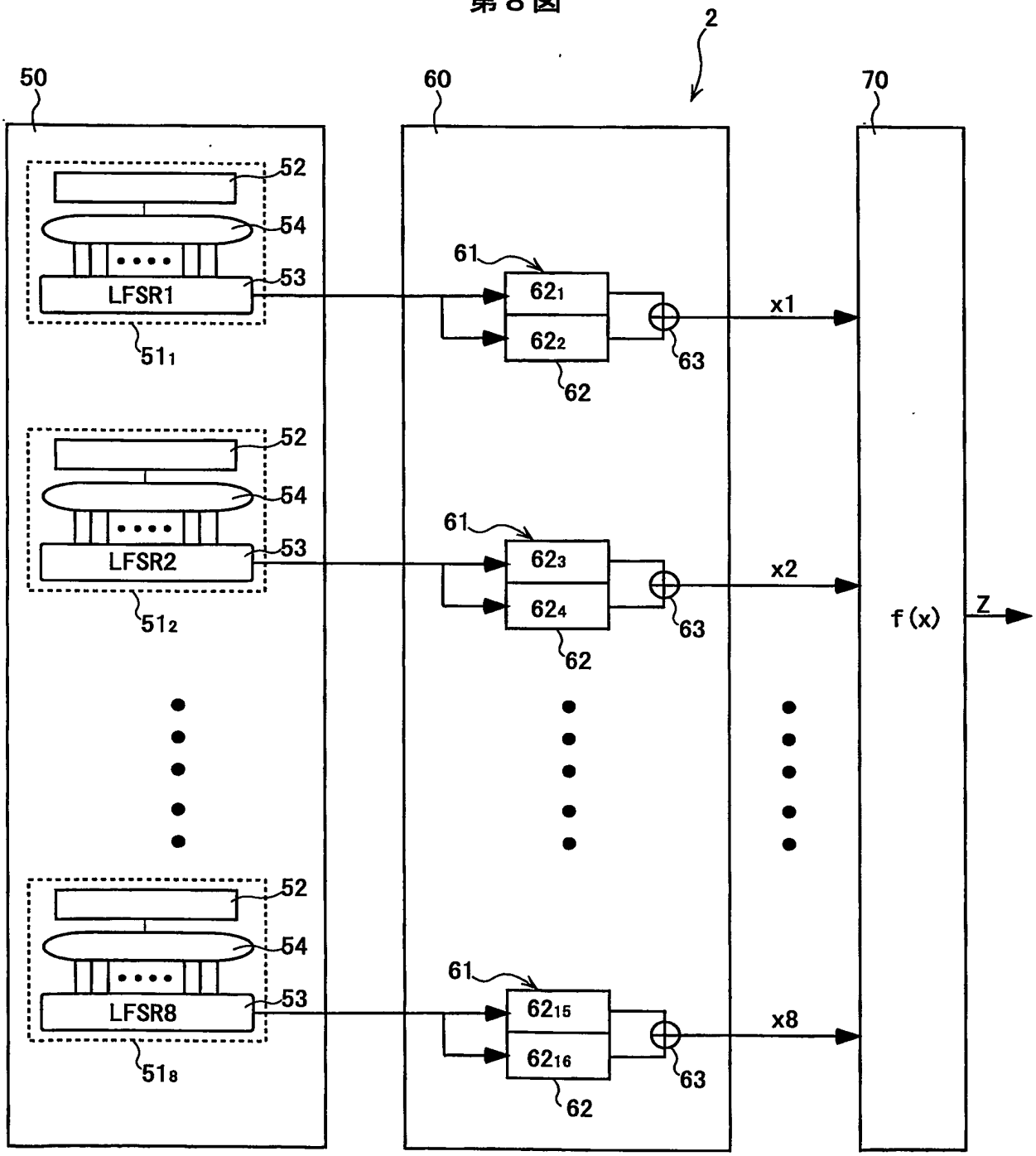
第２図

LFSR1	x^131+x^8+x^3+x^2+1
LFSR2	x^137+x^21+1
LFSR3	x^139+x^8+x^5+x^3+1
LFSR4	x^149+x^10+x^9+x^7+1
LFSR5	x^151+x^3+1
LFSR6	x^157+x^6+x^5+x^2+1
LFSR7	x^163+x^7+x^6+x^3+1
LFSR8	x^167+x^6+1

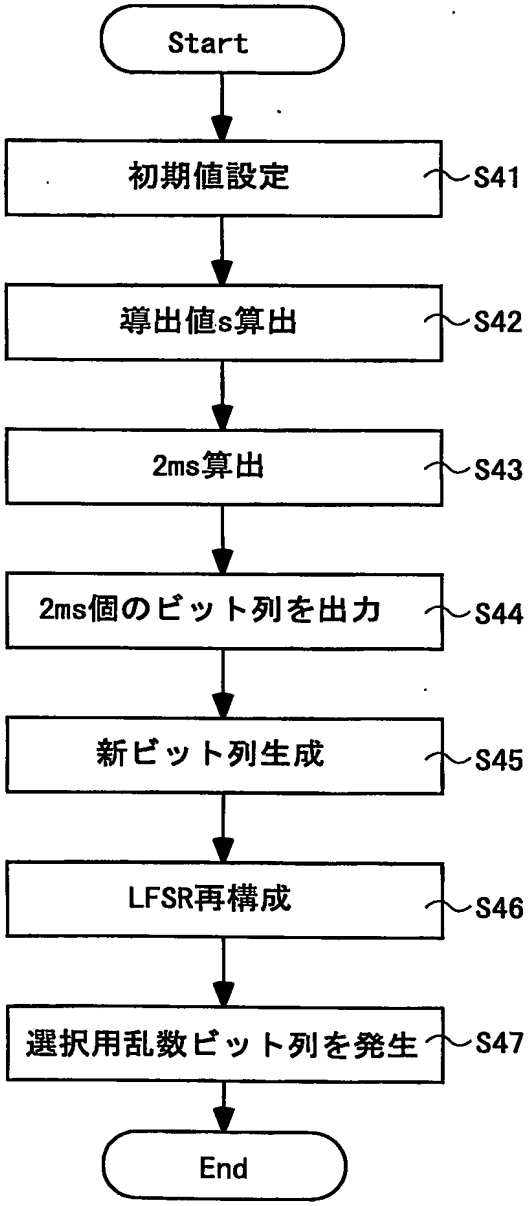
第４図


2
50
60
70
61
62_1
62_2
62_β
62
63
51_1
51_2
51_α
$62_{\beta+1}$
$62_{\beta+2}$
$62_{\beta+\beta}$
$62_{\alpha\beta-\beta+1}$
$62_{\alpha\beta-\beta+2}$
$62_{\alpha\beta}$
f(x)
Z

第８図


2
50
60
70
52
54
53
LFSR1
51₁
61
62₁
62₂
62
63
x1
LFSR2
51₂
62₃
62₄
x2
f(x)
Z
LFSR8
51₈
62₁₅
62₁₆
x8

第12図


Start
初期値設定
S41
導出値s算出
S42
2ms算出
S43
2ms個のビット列を出力
S44
新ビット列生成
S45
LFSR再構成
S46
選択用乱数ビット列を発生
S47
End